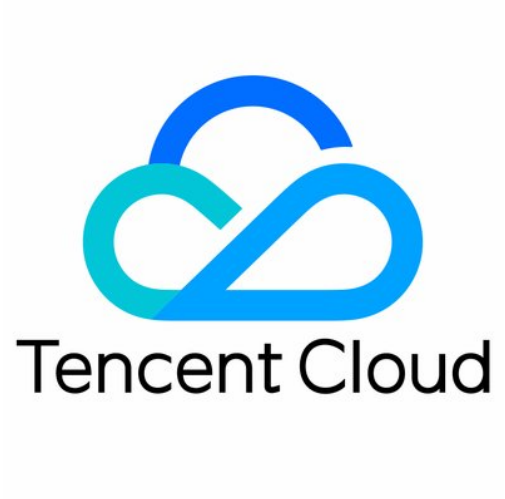
Tencent Cloud EdgeOne

Getting Started

Product Documentation



Contents

Getting Started
Choose business scenario

Last updated：2025-06-03 16:41:48

EdgeOne, based on edge nodes distributed across global availability zones, provides users with an all-in-one edge security acceleration platform service. It integrates a variety of rich capabilities, including static and dynamic CDN acceleration, Anti-DDoS, Web protection, Bot management, Layer 4 proxy, edge functions, Pages, media services, and DNS record management. It aims to offer comprehensive security protection and access acceleration services for websites, applications, apps, API interfaces, as well as TCP/UDP protocols.
Based on your business scenario, we recommend that you choose appropriate business types provided by EdgeOne, select suitable scenarios, and immediately connect your current business to EdgeOne, then enable the security acceleration service.

Business types provided	Supported capabilities	Mainly address problems	Common scenario examples
Website security acceleration	Provide rich features such as dynamic and static CDN acceleration, Web protection, Bot management, edge functions, and media services for websites/apps/businesses accessed via domain names.	Slow access speed in business: Users experience slow access speeds when accessing through different regions and operators, and are prone to buffering and access failures. Suffer from network attacks: There exist various types of network attacks in currently connected business, such as risk of being stolen, vulnerability attack, CC attack and Bot crawler. Poor server performance: The server bandwidth resource and performance of the site are limited. When a large number of users access it centrally, it will cause the origin server to be unable to host, resulting in users' access being unavailable.	For example: portal website, game download, popular video on demand, social forum, transaction/payment/login API, OTA upgrade and other scenarios.

	Provide L4 proxy acceleration for TCP/UDP requests and support providing exclusive DDoS protection.	Provide security acceleration for businesses that cannot be accessed via domain names, such as those based on Layer 4 forwarding.	For example: global office application acceleration, global game server co-location, TRTC connection and other business scenarios.
Pages	By importing Git repositories, using templates, or directly uploading, users can quickly build and deploy static sites and serverless applications. Additionally, with the capability of Edge functions, efficient content delivery and dynamic functionality expansion can be achieved to support fast access for global users.	**Deployment process is cumbersome:** The cycle from code writing to deployment and launch is long, making it difficult to ensure rapid iteration of projects, allowing companies to quickly respond to market demands. **Slow page access speed on sites:** Users find it hard to have a smooth experience during access, resulting in poor website performance. **Complex server deployment and high server-side development costs:** It requires self-configuration and management of servers and other infrastructure, making it impossible to directly write ultra-low-latency server logic at edge nodes.	For example: Personal blog, brand official website, event promotion page, AI integration application, documentation site, etc.

Quick access to website security acceleration

Last updated：2025-06-23 15:02:24

This document describes how to add a security acceleration site to Tencent Cloud EdgeOne and enable security acceleration, so that you can get a quick start with the EdgeOne service.

EdgeOne brings the following benefits to your security acceleration site:
EdgeOne nodes provide dynamic and static smart acceleration to enable users to obtain resources from nodes nearby, which avoids network issues due to cross-region or cross-ISP access.
Files are cached on nodes to reduce the proportion of origin-pull requests, which decreases the traffic to the origin.
Services are provided from EdgeOne nodes to hide the IP address of the origin and protect the origin from malicious attacks.
More EdgeOne capabilities, such as DNS, security protection, edge functions, and L4 proxy, can be integrated with your site.

Preparations

1. You have registered a Tencent Cloud account.
2. If your business currently uses a domain names for access, you need to prepare a registered domain, such as `example.com`. For more information about domain name registration, see Domain Registration.

Note:
If you want to set the service region of your site to **Chinese mainland** or **Global**, the domain name must have been filed with the Chinese Ministry of Industry and Information Technology. For more information,please refer to ICP Registration.

3. Your site is hosted on an accessible service, such as Cloud Virtual Machine (CVM) or Cloud Object Storage (COS). For example, you have built a cross-border e-commerce site based on Tencent Cloud CVM, and the current server IP address is: `1.1.1.1`.

Access site

Step 1: Add the Site

Perform the following operations to add the site to EdgeOne:
1. Log in to the EdgeOne console.
2. Perform different operations according to the following scenarios.
First-time console login

Adding sites after having other types of resources
If you are logging into the console for the first time, or you currently don't have any resources in EdgeOne, you will enter the scenario selection hall. On this interface, click **Add site**.

If you are adding a site for the first time but already have other resources, you can click the **Web Security Acceleration** tab at the top,

3. When adding a site, you need to access EdgeOne through the domain. If your business is purely L4 traffic, you can also choose to access without a domain name and use EdgeOne's L4 proxy service.
Domain access
No domain access
By default, EdgeOne requires you to use your current business's second-level domain as the site name for access. In the site input field, enter the site domain name you have prepared, for example: example.com. Click **Continue**.
Note:
Domain access enables your site to have complete web security acceleration capabilities. We recommend that you access through a domain name.

If your current business is not accessed through a domain name, you can also click **No domain Access** in the upper right corner to switch to the no-domain access mode. In this case, you only need to enter a custom site name and click **Continue**.

Step 2: Select Service Region and Plan

This step requires binding the site access plan specs so that the platform can allocate the corresponding service resources for you. You can bind by **purchase plan** or **bind sites to your plan**:
Purchase plan
Bind sites to your plan
1. When entering the plan selection, the default is the **Purchase plan** page. Currently. You can view the Comparison of EdgeOne Plans to see the differences between the different plan versions.

2. After confirming the plan, check and agree to the EdgeOne Service Level Agreement below, and click the next step.
1. If you have already purchased a plan, you can click **Bind sites to your plan** to switch to the binding plan page and select the purchased plan to bind.

2. After selecting the plan, check and agree to the EdgeOne Service Level Agreement below, and click **Next**.

Step 3: Select the Access Mode

If you are accessing through a domain name, this step requires you to select the acceleration region and access mode that meet your needs.

Note:

If you are accessing through No domain access, no operation is required for this step.

1. Select the acceleration region. The acceleration region is mainly used to allocate node resources for the current site. When you select the Chinese mainland availability zone and the Global availability zone, it is required that the current domain has completed the MIIT (Ministry of Industry and Information Technology) ICP Filing.

2. Select the access mode. EdgeOne provides you with two access modes, namely NS server access mode, CNAME access mode and DNSPod managed access. The differences between the different access modes are as follows:

Mode	NS Access (Recommended)	CNAME Access	DNSPod Managed Access
Scenario	You want to change the original DNS provider and host DNS on EdgeOne.	You have hosted the domain name to another DNS provider, such as Tencent Cloud DNSPod, and you do not want to change the DNS provider.	When the domain name is hosted on Tencent Cloud DNSPod, it is recommended to use this mode for access
Access mode	You only need to change the settings of the DNS server once at the original DNS provider. After that, you can easily enable secure acceleration for the domain name in the EdgeOne console.	Each time you add a new subdomain and enable secure acceleration, you must add a CNAME record at the corresponding DNS provider.	If the domain name is already hosted on Tencent Cloud DNSPod and is in effect, this mode is selected to complete access directly after backend verification by EdgeOne.
Verification method	You need to change the URLs of the original NS servers to the ones provided by EdgeOne.	You need to verify the domain name ownership by adding a DNS record or using the verification file.	No ownership verification is required.
Scheduling method	After secure acceleration is enabled for the domain name, the A record can be directly resolved to point to the nearest EdgeOne edge node.	After secure acceleration is enabled for the domain name, the client access is scheduled to the nearest EdgeOne node by using the CNAME record.	After secure acceleration is enabled for the domain name, it is scheduled to the nearest EdgeOne edge node via Cname.

NS Access
CNAME Access
DNSPod Managed Access
1. On the **Select an access mode** tab, select **NS access**.
2. (Optional) In NS Access mode, EdgeOne automatically scans all DNS records for the domain name. You can verify the scan results by comparing them with the original DNS records.
If all the original DNS resolution records are retrieved, clicking **Import all** to import them to EdgeOne.
If you find that some DNS resolution records are missing, click **Add record** or **Batch import** to add them.
3. Click **Next**. In the NS server access mode, you need to go to the original domain registration service provider and change the domain's DNS server address to the DNS server address provided by EdgeOne. The operation steps can be referred to: Modify DNS server.

4. After the change, EdgeOne automatically detects the current URLs of the NS servers. After settings of the NS servers take effect, click **OK**.
Note:
The process may be slow with some domain registrars, please be patient.
1. On the **Select an access mode** tab, select **CNAME access** and click **Next**.
2. Verify the site ownership. EdgeOne allows you to verify your site ownership through DNS verification or file verification. For more information, see Verifying Site Ownership.

3. After the site ownership is verified, click **OK**.
Note:
The prerequisite for using this mode is that your current domain name is already hosted on Tencent Cloud DNSPod and is in effect.
1. In the access mode options, select **DNSPod managed access** and click **Finish**.
2. When you use this mode for the first time, a pop-up window will remind you of authorization to use the TEO_QCSLinkedRoleInDnspodAccessEO service role permission. Click **Agree to Authorization**. After the authorization is successful, site access will be successfully completed.

Access security acceleration

Add an Acceleration Domain

Note:
If your current site is using No domain access, it only supports adding L4 proxy service.
1. Click the **Site List** in the left sidebar, and select the added **site** to go to Site Details Management.

2. Click **Domain Name Service** > **Domain Management** to go to the Domain Management Details page, and click **Add Domain Name** to add a new acceleration domain name.
3. Enter the acceleration domain name to be added and the corresponding origin server information. Once the configuration is complete, click **Next**.

Configuration item	Note
Acceleration domain name	Domain name provided for client access. Enter the host record value corresponding to the domain name. Wildcard domain name access is supported. If you need to access the main domain name, simply enter @. For example: If you need to accelerate the website `www.example.com`, enter `www` here.
Origin server configuration	The origin server is the final resource address accessed when the client initiates a request. You can choose from IP/domain name, COS origin server, and origin server group: **IP/domain name:** It is used to connect a single origin server. You can enter a single IP or a single domain name as the origin server. **COS origin server:** It is used to add Tencent Cloud COS and AWS S3 authentication compatible COS buckets as origin servers. If the bucket allows public read-write access, you can also connect directly using the origin server type of IP/domain name. Origin server group**:** If the origin server has multiple IPs, you can add them by configuring an origin server group. VOD**:** Buckets authorized in VOD can be set to apply to all files within the application or to files in a specific bucket. Load balancing**:** Actively detect origin server latency and health status, configure intelligent traffic scheduling policies, and provide safer and faster traffic distribution services. For example: There is an existing cross-border e-commerce website built using Tencent CVM. The IP address of the server is: `10.1.1.1`. When configuring the origin server, select the IP/domain name as origin server configuration and enter this server address. **Note:** 1. We recommend that you configure your origin server in the same region as the acceleration region. For instance, if the acceleration region is a Chinese mainland availability zone, set the origin server to be within the mainland for better origin-pull performance. If the origin server is in a global availability zone (excluding the Chinese mainland) and requires cross-border access, the origin-pull effect may not be guaranteed. If you need to accelerate access by Chinese mainland users and the origin site is in a global availability zone (excluding the Chinese mainland), refer toCross-regional Secure Acceleration (Oversea Sites). 2. If your acceleration region is a global availability zone, you can add corresponding rules in the rule engine. Set the matching condition to client geographic location and choose to modify the origin server, directing origin-pull requests to different origin servers based on the regions to ensure the origin-pull effect.

	3. Do not enter an acceleration domain name that has already been connected to EdgeOne and whose origin server points to the current domain name as the origin server address. Doing so may cause a loop in resolution, preventing normal origin-pull.
IPv6 access	You can choose whether to enable IPv6 access support. Refer to the document: IPv6 Access. The default is to follow site configuration.
Origin-pull protocol	You can select the access protocol supported by your origin server. The default is to follow the protocol. The options are as follows: **Follow protocol:** The origin-pull protocol is the same as the user access request protocol. **HTTP**: The HTTP protocol is used for origin-pull. **HTTPS:** The HTTPS protocol is used for origin-pull.
Origin-pull port	It is used to specify the port used for origin-pull. Make sure that the port specified on your origin server is accessible. By default, HTTP origin-pull uses port 80, and HTTPS origin-pull uses port 443.
Origin HOST header	If your origin server hosts multiple sites and you need to specify which site to access via the origin HOST header, you can select one of the following options when the origin type is IP/domain: Use acceleration domain name: Use the acceleration domain as the origin HOST header; Use origin domain name: Use the origin domain as the origin HOST header. If the origin address is an IP address, this option is not available; Custom: Customize the origin HOST header used when requesting resources from the origin server.

4. (Optional) When a domain name is added, EdgeOne provides recommended configuration based on common service scenarios to ensure smoother and safer operation. You can select recommended configuration based on your service scenario, click **Next** to apply the configuration or directly click **Skip** to proceed without applying any configuration, and go to the next step.

5. Once a domain name is created, EdgeOne will assign a CNAME address to the domain name. You need to complete the CNAME configuration to enable the secure acceleration for the domain name. For the configuration method, refer to: Modification of CNAME Resolution.

Note:

Prior to transitioning your access method, it is advisable to consult the Verify Business Access section to ascertain the accuracy of your current domain configuration.

Should there be a necessity to configure an HTTPS certificate for your domain, upon the completion of domain deployment, you may refer to Deploying/Updating SSL Managed Certificates to EdgeOne Domains for configuration guidance.

Adding L4 proxy service

L4 proxy is the acceleration service of EdgeOne based on TCP/UDP. By leveraging widely distributed layer-4 proxy nodes, unique DDoS module, and smart routing technology, EdgeOne implements nearby access for end users, edge traffic cleansing, and port monitoring and forwarding. It thus offers high-availability and low-latency DDoS mitigation and acceleration services for layer-4 applications.You can enable TCP/UDP protocol acceleration and security protection features on the L4 proxy page. For details, see Create L4 proxy instance.

Note:

The L4 proxy is only available with the Enterprise Edition package.

Enable Security Protection On Demand

EdgeOne provides flexible and configurable DDoS protection and Web Protection capabilities, supporting diverse security policy configurations and security event alert options, helping you verify traffic and requests at the edge to prevent external attacks and security risks from affecting your business and sensitive data. You can enable these features on demand according to your business needs, providing comprehensive Web Protection services for websites/apps/applications and other Web businesses to defend against application layer attacks and block malicious requests; enable DDoS protection for UDP/TCP L4 businesses to resist network layer distributed attacks. For details, seeDDoS Protection and Web Protection Overview.

For No Domain Sites, Configure Domain Names to Enable More Security Acceleration Features

If during usage, your domainless site needs to bind a domain name to use more security acceleration features, you can go to the Domain Management page, click to set site domain name, and use NS/CNAME/DNSPod mode to access EdgeOne.

Learn More

EdgeOne Overview
Rule Engine Overview
Edge Functions Overview
Web Protection Overview
DDoS Protection Overview

Quick deploying a website with Pages

Last updated：2025-06-14 13:18:47

This guide will walk you through how to quickly create and deploy a website using Pages, helping you get started with the Pages service.
Pages is a front-end development and deployment platform built on the Tencent EdgeOne infrastructure, specifically designed for modern Web development. It helps developers quickly build and deploy static sites and serverless applications. By integrating Edge functions capabilities, it achieves efficient content delivery and dynamic functionality extension, supporting fast access for global users.

Step 1: Choose a Creation Method

After completing the preparation work, you can begin connecting to EdgeOne.
1. Log in to the EdgeOne console.
2. Choose how to create your Pages project based on the following scenarios:
First-time Console Login
Creating Projects After Having Other Resources
If you're logging into the console for the first time or currently have no resources in EdgeOne, you'll enter the scenario selection hall. On this interface, hover over **Create Project** and choose from three methods: "Import Git Repository," "Start from Template," or "Upload directly."

If you're creating a Pages project for the first time but already have other resources, you can click the Pages Tab at the top and select how to create your Pages project in that tab.

Creation Method	Description
Import Git Repository	Requires connection to a Git repository provider to import code and create a website from the Git repository.
Start from Template	You can quickly create a website using EdgeOne's pre-made templates.
Upload directly	You can upload your current project code to EdgeOne and deploy your site based on the uploaded content.Note: If you choose to upload files, your current project cannot switch to Git integration. You must create a new project with Git integration to use automatic deployment.

Step 2: Connect to Git Repository

> **Note:**
> If you chose "Upload directly" as your creation method, you can skip this step and proceed to Step 3.

When you select "Import Git Repository" or "Start from Template," you need to connect to your current Git provider. Currently supported Git providers include Github, Gitee, and others. Here's an example using Github:
1. On the console page, click "Github" to link your repository.

2. Grant EdgeOne permission to access your repositories by clicking **Authorize EO Pages**.

3. Select the repository you want to deploy or authorize all repositories, then click **Install**.

Step 3: Customize Build

The build process differs depending on the creation method you chose:
Import Git Repository
Start from Template
Upload directly
After connecting to a Git repository, you need to configure the build settings. This step is crucial for correctly compiling and successfully deploying your project.
1. Select the repository you want to deploy.

2. Enter your build commands. If you're unsure, check the scripts section in your package.json file. When selecting an acceleration region, different regions determine the node resources allocated to your project and whether ICP filing is required when adding a custom domain. For details, refer to Domain Management - Acceleration Region.

3. Review your configuration, and once confirmed, click **Start Deployment**. Pages will automatically build your project and deploy it to the global edge network.
We offer a variety of templates for different use cases. Below, we'll show you how to quickly launch and deploy a project using a template. Later, you can develop based on our templates with continuous builds and deployments.
1. After authorizing Github, select a template you want to deploy.

2. Set up the project name and repository name, and adjust repository properties if needed. When selecting an acceleration region, different regions determine the node resources allocated to your project and whether ICP filing is required when adding a custom domain. For details, refer to Domain Management - Acceleration Region.

3. Click **Create Now**, and we'll create a repository in your GitHub account based on the template. The deployment process will start automatically. You can clone this repository locally for further development and push changes as needed.
You can directly upload your built project assets to Pages and deploy them to EdgeOne's global network. If you want to integrate with your own build platform or upload from your local computer, you should choose direct upload rather than importing from a Git repository.
1. After selecting "Direct Upload" when creating your project, you'll see the following page.

2. After filling in the "Project Name" and "Acceleration Region," drag and drop your project assets to the designated area.

3. Click **Start Deployment**. After the assets are uploaded, the project will be created and you'll be directed to the deployment details page. Once deployment is successful, you can view your project through the preview link.

Step 4: Verify Deployment Status

When deployment is complete, you'll see the following image indicating successful deployment!

You can generate a deployment preview link by clicking the **Preview** button in the upper right corner of the Build & Deploy menu to access that version's page content.

You can also generate a project preview link by clicking the "Preview" button in the upper right corner of the "Project Overview" page to access the latest version of the page content.

How to Add a Custom Domain

After verifying that the preview content is correct, we strongly recommend that you immediately add a custom domain for access to ensure your project appears more professional and trustworthy during long-term access. For detailed information on how to add a custom domain, please refer to the Domain Management - Custom Domain section.

How to Create a New Deployment

The process for creating a new deployment varies depending on how you initially created your project:
Import Git Repository/Start from Template
Upload directly
When a new commit is pushed to the main branch, EdgeOne will automatically pull and deploy the latest commit.

You can also use the "Redeploy" button in the Build & Deploy list to create a new deployment using the same source code as the current deployment with the latest project configuration.

You can deploy a new version through the "New Deployment" option on the Build & Deploy page.

Drag and drop the new version of your project assets to the designated area. The deployment environment defaults to "Production Environment" but can be switched to "Preview Environment."

Note:
Production Environment: Updates the live website that users access, effective immediately.
Preview Environment: Validate changes in an isolated environment without affecting official data.

Troubleshooting

If the deployed version differs from the repository, make sure to pull the latest version.
If a 404 error occurs after a successful direct upload deployment, check if there is an index.html file in the root directory of the uploaded folder.
If you have other issues, refer to our Troubleshooting Guide, or scan the "Developer Communication Group" QR code in the upper right corner to join the group and contact us.